CLAIM AMENDMENTS

This listing of claims will replace all prior versions and listings of claims in the application.

Listing of the Claims:

1-25. (Canceled)

26. (Currently Amended) A method of controlling traffic on a data network, said traffic comprising payload data and associated signaling data, the method comprising:

reading a portion of said payload data for a first traffic of a first communications session between a first entity and a second entity communicating over said data network;

~~determining~~ using a signature in the portion of the payload data to determine whether said portion of the payload data identifies ~~a traffic content type~~ peer-to-peer (P2P) traffic;

storing signaling data associated with said portion of the payload data;

reading signaling data for a second traffic of a ~~further or resumed~~ second communications session on said data network; ~~and~~

comparing said read signaling data with said stored signaling data to identify said second traffic as ~~a further~~ the P2P traffic ~~of said controlled traffic content type~~; and

controlling said ~~further or resumed~~ second communications session responsive to said identification of the P2P traffic, by limiting propagation of the P2P traffic without limiting propagation of non-P2P traffic.

27. (Currently Amended) ~~A method as claimed in~~ The method of claim 26, wherein said controlling further comprises:

controlling a route of said ~~further or resumed~~ second communications session traffic.

28. (Currently Amended) ~~A method as claimed in~~ The method of claim 26, further comprising:

~~wherein said reading of signaling~~ data for the second traffic includes

reading at least a portion of said signaling data for said second traffic;~~,~~

~~wherein said method includes~~

determining from said signaling data an address of an originator of said ~~further or resumed~~ second communications session, said originator comprising one of said first and second entities;[[,]] and ~~wherein said method comprises~~

sending a signal to said originator using said determined address.

29. (Currently Amended) ~~A method as claimed in~~ The method of claim 26, wherein said controlling further comprises:

signaling with said signaling data.

30. (Currently Amended) ~~A method as claimed in~~ The method of claim 26, wherein said controlling further comprises:

sending a message in said payload data.

31. (Currently Amended) ~~A method as claimed in~~ The method of claim 30, wherein said message includes a request to retry establishing said ~~further or resumed~~ second communications session.

32. (Currently Amended) ~~A method as claimed in~~ The method of claim 26, wherein said storing is responsive to said determining.

33. (Currently Amended) ~~A method as claimed in~~ The method of claim 26, wherein said reading of the portion of said payload data for the first traffic further comprises:

reading first payload data for a communication from said first to said second entity and second payload data for a communication from said second to said first entity, and wherein said determining whether said portion of payload data

identifies ~~a controlled traffic content type~~ the P2P traffic; and

determines whether both said first and said second payload data ~~are of said controlled traffic content type~~ contain the P2P traffic.

34. (Currently Amended) ~~A method as claimed in~~ The method of claim 33, further comprising

buffering said first and second payload data for said determining.

35. (Canceled).

36. (Currently Amended) ~~A method as claimed in~~ The method of claim 26, further comprising:

signaling, responsive to said determining, to at least one of said first and second entities to interrupt said communications session.

37. (Currently Amended) ~~A method as claimed in~~ The method of claim 26, wherein said second traffic comprises an attempt to begin a further communications session of ~~said controlled traffic content type~~ the P2P traffic or to resume said communications session, and wherein said controlling further comprises:

controlling traffic of said ~~further or resumed~~ second communications session.

38. (Currently Amended) ~~A method as claimed in~~ The method of claim 26, wherein said network comprises a packet data network and wherein said signaling data includes a destination identifier.

39. (Currently Amended) ~~A method as claimed in~~ The method of claim 38, wherein said network comprises an internet protocol (IP) network~~, in particular a transmission control protocol (TCP) IP network,~~ and wherein said signaling data includes a destination address and port number.

40. (Currently Amended) ~~A method as claimed in~~ The method of claim 26, wherein said traffic content type to be controlled includes ~~peer-to-peer~~ P2P protocol network traffic employing a variable TCP port number for ~~peer-to-peer~~ P2P connections.

41. (Currently Amended) ~~A method as claimed in~~ The method of claim 40, wherein said controlling further comprises:

routing said ~~peer-to-peer~~ P2P traffic to a ~~peer-to-peer~~ P2P network gateway.

42. (Currently Amended) ~~A method as claimed in~~ The method of claim 40, wherein said controlling further comprises:

routing said ~~peer-to-peer~~ P2P traffic to a ~~peer-to-peer~~ P2P network cache.

43-44. (Canceled)

45. (Currently Amended) A router for controlling traffic on a data network, said traffic comprising payload data and associated signaling data, the router comprising:

a network interface ~~for interfacing t~~hat interfaces with said data network;

a packet switch coupled to the network interface that separates the traffic into peer-to-peer (P2P) traffic and non P2P traffic, wherein propagation of the P2P traffic is limited without limiting propagation of the non P2P traffic;

a data memory ~~operable to store t~~hat stores data to be processed;

an instruction memory ~~storing t~~hat stores computer executable code; and

a processor coupled to said network interface, to said data memory, and to said instruction memory ~~and operable to process t~~hat processes said data in accordance with the computer-executable code stored in said instruction memory, whereby said processor is configured to:

read a portion of said payload data for a first traffic of a communications session between a first entity and a second entity communicating over said network;

using a signature in the portion of the payload data to determine whether said portion of payload data identifies ~~a t~~he P2P traffic ~~content type to be controlled~~;

store signaling data associated with said portion of payload data;

read signaling data for a second traffic on said network; ~~and t~~o

compare said read signaling data with said stored signaling data to identify an attempt to begin a ~~further~~ second communications session of said ~~controlled~~ P2P traffic ~~type or to resume said communications session~~; and

control said ~~further or resumed~~ second communications session responsive to said identification.

46. (Currently Amended) ~~A router as claimed in~~ The router of claim 45, wherein network comprises a packet data network, wherein said signaling data comprises a destination identifier to identify a destination of a packet of data comprising said first traffic, and wherein said storing stores a destination identifier for said first traffic ~~of said controlled traffic content type~~ that is the P2P traffic in said data memory responsive to identifying said ~~controlled~~ P2P traffic ~~content type~~.

47. (Currently Amended) ~~A router as claimed in~~ The router of claim 46, wherein said processor is further configured to:

store portions of said payload data of said communications session sent from both said first and said second entity; and

determine when communications from both said first and second entities are ~~of a said controlled~~ the P2P traffic ~~content type~~.

48-52. (Canceled).